

RING CLASS INVARIANTS OVER IMAGINARY QUADRATIC FIELDS

ICK SUN EUM, JA KYUNG KOO, AND DONG HWA SHIN

ABSTRACT. We show by adopting Schertz's argument with the Siegel-Ramachandra invariants that the singular values of certain Δ -quotients generate ring class fields over imaginary quadratic fields.

1. INTRODUCTION

In number theory ring class fields over imaginary quadratic fields, more exactly, primitive generators of ring class fields as real algebraic integers play an important role in the study of certain quadratic Diophantine equations. For example, let n be a positive integer and $H_{\mathcal{O}}$ be the ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$. If p is an odd prime not dividing n , then we have the following assertion:

$p = x^2 + ny^2$ is solvable for some integers x and y
 \iff the Legendre symbol $(-n/p) = 1$ and $f_n(X) \equiv 0 \pmod{p}$ has an integer solution, where $f_n(X)$ is the minimal polynomial of a real algebraic integer α which generates $H_{\mathcal{O}}$ over K ([4, Theorem 9.2]).

Given an imaginary quadratic field K with the ring of integer $\mathcal{O}_K = \mathbb{Z}[\theta]$ such that $\theta \in \mathfrak{H}$ (= the complex upper half-plane), let $\mathcal{O} = [N\theta, 1]$ be the order of conductor N (≥ 1) in K . We know a classical result from the theory of complex multiplication that the j -invariant $j(\mathcal{O}) = j(N\theta)$ generates the ring class field $H_{\mathcal{O}}$ over K ([4, Theorem 11.1] or [12, Chapter 10 Theorem 5]). We have an algorithm to find the minimal polynomial (= class polynomial) of such a generator $j(\mathcal{O})$ ([4, §13.A]), however, its coefficients are too gigantic to handle for practical use.

Unlike the classical case, Chen-Yui ([1]) constructed a generator of the ring class field of certain conductor in terms of the singular value of the Thompson series which is a Hauptmodul for $\Gamma_0(N)$ or $\Gamma_0^{\dagger}(N)$, where $\Gamma_0(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N}\}$ and $\Gamma_0^{\dagger}(N) = \langle \Gamma_0(N), \begin{pmatrix} 0 & -1/\sqrt{N} \\ \sqrt{N} & 0 \end{pmatrix} \rangle$ in $\mathrm{SL}_2(\mathbb{R})$. In like manner, Cox-Mckay-Stevenhagen ([5]) showed that certain singular value of a Hauptmodul for $\Gamma_0(N)$ or $\Gamma_0^{\dagger}(N)$ with rational

2000 *Mathematics Subject Classification.* Primary 11G16; Secondary 11F03, 11G15, 11R37.

Key words and phrases. Class field theory, complex multiplication, elliptic and modular units, modular functions.

This research was partially supported by Basic Science Research Program through the NRF of Korea funded by MEST (2010-0001654). The third named author is partially supported by TJ Park Postdoctoral Fellowship.

Fourier coefficients generates $H_{\mathcal{O}}$ over K . And, Cho-Koo ([2, Corollaries 4.4 and 4.5]) recently revisited and extended these results by using the theory of Shimura's canonical models and his reciprocity law.

On the other hand, Ramachandra ([13, Theorem 10]) showed that arbitrary finite abelian extension of an imaginary quadratic field K can be generated over K by a theoretically beautiful elliptic unit, but his invariant involves overly complicated product of high powers of singular values of the Klein forms and singular values of the Δ -function to use in practice. This motivates our work of finding simpler ring class invariants in terms of the Siegel-Ramachandra invariant as Lang pointed out in his book ([12, p.292]) in case of ray class fields.

More precisely, for any pair $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ we define the *Siegel function* $g_{(r_1, r_2)}(\tau)$ on \mathfrak{H} by the following infinite product

$$g_{(r_1, r_2)}(\tau) = -q^{(1/2)\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)} (1 - q_z) \prod_{n=1}^{\infty} (1 - q^n q_z) (1 - q^n q_z^{-1}), \quad (1.1)$$

where $\mathbf{B}_2(X) = X^2 - X + 1/6$ is the second Bernoulli polynomial, $q = e^{2\pi i \tau}$ and $q_z = e^{2\pi i z}$ with $z = r_1 \tau + r_2$. As the singular values of Siegel functions we shall define the Siegel-Ramachandra invariants in §2. And, by adopting Schertz's idea ([14, Proof of Theorem 3]) we shall determine certain class fields over K generated by norms of the Siegel-Ramachandra invariants (Theorem 2.7). In the case of ring class fields we are enable to express the norms as the singular values of certain Δ -quotients (Theorem 4.2), where

$$\Delta(\tau) = (2\pi i)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}. \quad (1.2)$$

For example, let $N = \prod_{k=1}^n p_k^{e_k}$ be a product of odd primes p_k which are inert or ramified in K/\mathbb{Q} . We assume that

$$e_k + 1 > 2/r_k \quad (k = 1, \dots, n) \quad \text{and} \quad \begin{cases} \gcd(p_1, \omega_K) = 1 & \text{if } n = 1 \\ \gcd(\prod_{k=1}^n p_k, \prod_{k=1}^n (p_k^{2/r_k} - 1)) = 1 & \text{if } n \geq 2, \end{cases}$$

where r_k is the ramification index of p_k in K/\mathbb{Q} and ω_K is the number of roots of unity in K . Then, certain quotient of the singular values $\Delta((N/N_S)\theta)$, where N_S are the products of p_k 's, becomes a generator of the ring class field of the order $[N\theta, 1]$ over K (Remark 4.3). This result is a continuation of our previous work with $n = 1$ ([7, §5]).

Note that Theorems 2.7 and 4.2 heavily depend on Lemma 2.5 which requires the assumption (2.3). However, in §5 we shall develop a lemma which substitutes for Lemma 2.5 in order to release from the assumption (2.3) to some extent (Lemma 5.3 and Remark 5.5). For example, let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$, and N (≥ 2) be an integer with prime factorization $N = \prod_{a=1}^A s_a^{u_a} \prod_{b=1}^B q_b^{v_b} \prod_{c=1}^C r_c^{w_c}$, where each s_a (respectively, q_b and r_c) splits (respectively, is inert and ramified) in K/\mathbb{Q} . If

$$4 \sum_{a=1}^A \frac{1}{(s_a - 1)s_a^{u_a - 1}} + 2 \sum_{b=1}^B \frac{1}{(q_b + 1)q_b^{v_b - 1}} + 2 \sum_{c=1}^C \frac{1}{r_c^{w_c}} < 1,$$

then one can also apply Theorem 4.2 without assuming (2.3) (Theorem 5.4 and Remark 5.5).

Lastly, by making use of our simple invariant developed in Theorem 4.2 we shall present three examples (Examples 4.4, 4.5 and 5.6).

2. PRIMITIVE GENERATORS OF CLASS FIELDS

In this section we shall investigate some class fields over imaginary quadratic fields generated by norms of the Siegel-Ramachandra invariants.

For a given imaginary quadratic field K we let

- d_K : the discriminant of K ,
- \mathfrak{d}_K : the different of K/\mathbb{Q} ,
- \mathcal{O}_K : the ring of integers of K ,
- ω_K : the number of root of unity in K ,
- I_K : the group of fractional ideals of K ,
- P_K : the subgroup of I_K consisting of principal ideals of K .

And, for a nonzero integral ideal \mathfrak{f} of K we set

- $I_K(\mathfrak{f})$: the subgroup of I_K consisting of ideals relatively prime to \mathfrak{f} ,
- $P_{K,1}(\mathfrak{f})$: the subgroup of $I_K(\mathfrak{f}) \cap P_K$ generated by the principal ideals $\alpha\mathcal{O}_K$ for which $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv 1 \pmod{\mathfrak{f}}$,
- $\text{Cl}(\mathfrak{f})$: the ray class group (modulo \mathfrak{f}), namely, $I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f})$,
- C_0 : the unit class of $\text{Cl}(\mathfrak{f})$,
- $\omega(\mathfrak{f})$: the number of roots of unity in K which are $\equiv 1 \pmod{\mathfrak{f}}$,
- $N(\mathfrak{f})$: the smallest positive integer in \mathfrak{f} .

By the *ray class field $K_{\mathfrak{f}}$ modulo \mathfrak{f} of K* we mean a finite abelian extension of K whose Galois group is isomorphic to $\text{Cl}(\mathfrak{f})$ via the Artin map σ , namely

$$\sigma = \left(\frac{K_{\mathfrak{f}}/K}{\cdot} \right) : \text{Cl}(\mathfrak{f}) \xrightarrow{\sim} \text{Gal}(K_{\mathfrak{f}}/K).$$

In particular, if $\mathfrak{f} = \mathcal{O}_K$, then we simply denote $K_{\mathfrak{f}}$ by H and call it the *Hilbert class field of K* . We have a short exact sequence

$$1 \longrightarrow \pi_{\mathfrak{f}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}}(\mathcal{O}_K^*) \xrightarrow{\Phi_{\mathfrak{f}}} \text{Cl}(\mathfrak{f}) \longrightarrow \text{Cl}(\mathcal{O}_K) \longrightarrow 1, \quad (2.1)$$

where

$$\pi_{\mathfrak{f}} : \mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{f}$$

is the natural surjection and $\Phi_{\mathfrak{f}}$ is induced by the homomorphism

$$\begin{aligned} \tilde{\Phi}_{\mathfrak{f}} : \pi_{\mathfrak{f}}(\mathcal{O}_K)^* &\longrightarrow \text{Cl}(\mathfrak{f}) \\ \pi_{\mathfrak{f}}(x) &\mapsto [x\mathcal{O}_K], \text{ the class containing } x\mathcal{O}_K, \end{aligned}$$

whose kernel is $\pi_{\mathfrak{f}}(\mathcal{O}_K^*)$ ([3, Proposition 3.2.3]).

Let χ be a character of $\text{Cl}(\mathfrak{f})$. We denote by \mathfrak{f}_{χ} the conductor of χ , namely

$$\mathfrak{f}_{\chi} = \gcd(\mathfrak{g} : \chi = \psi \circ (\text{Cl}(\mathfrak{f}) \rightarrow \text{Cl}(\mathfrak{g}))) \text{ for some character } \psi \text{ of } \text{Cl}(\mathfrak{g}),$$

and let χ_0 be the proper character of $\text{Cl}(\mathfrak{f}_\chi)$ corresponding to χ . Similarly, if χ' is any character of $\pi_{\mathfrak{f}}(\mathcal{O}_K)^*$, then the conductor $\mathfrak{f}_{\chi'}$ of χ' is defined by

$$\mathfrak{f}_{\chi'} = \gcd(\mathfrak{g} : \chi' = \psi' \circ (\pi_{\mathfrak{f}}(\mathcal{O}_K)^* \rightarrow \pi_{\mathfrak{g}}(\mathcal{O}_K)^*) \text{ for some character } \psi' \text{ of } \pi_{\mathfrak{g}}(\mathcal{O}_K)^*).$$

For a character χ of $\text{Cl}(\mathfrak{f})$ we denote by $\tilde{\chi}$ the character of $\pi_{\mathfrak{f}}(\mathcal{O}_K)^*$ defined by

$$\tilde{\chi} = \chi \circ \tilde{\Phi}_{\mathfrak{f}}.$$

If $\mathfrak{f} = \prod_{k=1}^n \mathfrak{p}_k^{e_k}$, then from the Chinese remainder theorem we have an isomorphism

$$\iota : \prod_{k=1}^n \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \xrightarrow{\sim} \pi_{\mathfrak{f}}(\mathcal{O}_K)^*,$$

and natural injections and surjections

$$\iota_k : \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \hookrightarrow \prod_{\ell=1}^n \pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^* \quad \text{and} \quad v_k : \prod_{\ell=1}^n \pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^* \rightarrow \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \quad (k = 1, \dots, n),$$

respectively. Furthermore, we consider the characters $\tilde{\chi}_k$ of $\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*$ defined by

$$\tilde{\chi}_k = \tilde{\chi} \circ \iota \circ \iota_k \quad (k = 1, \dots, n).$$

Lemma 2.1. *The notation being as above, we have*

- (i) $\mathfrak{f}_{\tilde{\chi}} = \mathfrak{f}_\chi$.
- (ii) $\tilde{\chi} \circ \iota = \prod_{k=1}^n \tilde{\chi}_k \circ v_k$.
- (iii) If $\tilde{\chi}_k \neq 1$, then $\mathfrak{p}_k \mid \mathfrak{f}_{\tilde{\chi}}$.

Proof. (i) and (ii) are immediate by the definitions of conductors and $\tilde{\chi}$, $\tilde{\chi}_k$, ι , v_k .

(iii) Without loss of generality we may assume $\tilde{\chi}_n \neq 1$. Suppose on the contrary $\mathfrak{p}_n \nmid \mathfrak{f}_{\tilde{\chi}}$. Then, by the definition of $\mathfrak{f}_{\tilde{\chi}}$ there is a character ψ' of $\text{Cl}(\mathfrak{f}_{\tilde{\chi}})$ which makes the following diagram commutative:

$$\begin{array}{ccc} \prod_{k=1}^n \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* & \xrightarrow{A} & \prod_{k=1}^{n-1} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \cong \pi_{\mathfrak{f}\mathfrak{p}^{-e_n}}(\mathcal{O}_K)^* \\ \downarrow \iota & & \downarrow B \\ \pi_{\mathfrak{f}}(\mathcal{O}_K)^* & \xrightarrow{C} & \pi_{\mathfrak{f}_{\tilde{\chi}}}(\mathcal{O}_K)^* \\ \downarrow \tilde{\chi} & & \downarrow \psi' \\ & \mathbb{C}^* & \end{array}$$

where A , B and C are natural surjections. If σ_n is an element of $\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*$ such that $\tilde{\chi}_n(\sigma_n) \neq 1$, then

$$\begin{aligned} 1 &\neq \tilde{\chi}_n(\sigma_n) = \tilde{\chi} \circ \iota \circ \iota_n(\sigma_n) = \tilde{\chi} \circ \iota(1, \dots, 1, \sigma_n) \\ &= (\psi' \circ C) \circ \iota(1, \dots, 1, \sigma_n) = \psi' \circ B \circ A(1, \dots, 1, \sigma_n) = \psi' \circ B(1, \dots, 1) = 1, \end{aligned}$$

which renders a contradiction. Therefore, $\mathfrak{p}_n \mid \mathfrak{f}_{\tilde{\chi}}$. \square

If $\mathfrak{f} \neq \mathcal{O}_K$ and $C \in \text{Cl}(\mathfrak{f})$, we take any integral ideal \mathfrak{c} in C . Let $\mathfrak{f}\mathfrak{c}^{-1} = [z_1, z_2]$ with $z = z_1/z_2 \in \mathfrak{H}$. We define the *Siegel-Ramachandra invariant* (of conductor \mathfrak{f} at C) by

$$g_{\mathfrak{f}}(C) = g_{(a/N(\mathfrak{f}), b/N(\mathfrak{f}))}(z)^{12N(\mathfrak{f})},$$

where a, b are integers such that $1 = (a/N(\mathfrak{f}))z_1 + (b/N(\mathfrak{f}))z_2$. This value depends only on the class C and belongs to the ray class field $K_{\mathfrak{f}}$ ([10, Chapter 2 Proposition 1.3 and Chapter 11 Theorem 1.1]). And, there is a well-known transformation formula

$$g_{\mathfrak{f}}(C_1)^{\sigma(C_2)} = g_{\mathfrak{f}}(C_1 C_2) \quad (C_1, C_2 \in \text{Cl}(\mathfrak{f})) \quad (2.2)$$

([10, p.236]).

For a nontrivial character χ of $\text{Cl}(\mathfrak{f})$ with $\mathfrak{f} \neq \mathcal{O}_K$, we define the *Stickelberger element* as

$$S_{\mathfrak{f}}(\chi, g_{\mathfrak{f}}) = \sum_{C \in \text{Cl}(\mathfrak{f})} \chi(C) \log |g_{\mathfrak{f}}(C)|,$$

and consider the *L-function*

$$L_{\mathfrak{f}}(s, \chi) = \sum_{\mathfrak{a} \neq 0 : \text{integral ideals of } K} \frac{\chi(\mathfrak{a})}{\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{a})^s} \quad (s \in \mathbb{C}).$$

From the second Kronecker limit formula ([12, Chapter 22 Theorem 1]) we get the following proposition.

Proposition 2.2. *The notation being as above, if $\mathfrak{f}_{\chi} \neq \mathcal{O}_K$, then*

$$\prod_{\mathfrak{p}|\mathfrak{f}, \mathfrak{p} \nmid \mathfrak{f}_{\chi}} (1 - \overline{\chi}_0(\mathfrak{p})) L_{\mathfrak{f}_{\chi}}(1, \chi_0) = \frac{\pi}{3\omega(\mathfrak{f})N(\mathfrak{f})\tau(\overline{\chi}_0)\sqrt{|d_K|}} S_{\mathfrak{f}}(\overline{\chi}, g_{\mathfrak{f}}),$$

where

$$\tau(\overline{\chi}_0) = - \sum_{\substack{x \in \mathcal{O}_K \\ x \bmod \mathfrak{f} \\ \gcd(x\mathcal{O}_K, \mathfrak{f}_{\chi}) = \mathcal{O}_K}} \overline{\chi}_0([x\gamma\mathfrak{d}_K\mathfrak{f}_{\chi}]) e^{2\pi i \text{Tr}_{K/\mathbb{Q}}(x\gamma)}$$

with γ any element of K such that $\gamma\mathfrak{d}_K\mathfrak{f}_{\chi}$ is an integral ideal relatively prime to \mathfrak{f} .

Proof. See [12, Chapter 22 Theorem 2] and [10, Chapter 11 Theorem 2.1]. \square

Remark 2.3. (i) The product factor $\prod_{\mathfrak{p}|\mathfrak{f}, \mathfrak{p} \nmid \mathfrak{f}_{\chi}} (1 - \overline{\chi}_0(\mathfrak{p}))$ is called the *Euler factor* of χ . If there is no such \mathfrak{p} with $\mathfrak{p}|\mathfrak{f}$ and $\mathfrak{p} \nmid \mathfrak{f}_{\chi}$, then it is understood to be 1.

(ii) As is well-known, $L_{\mathfrak{f}_{\chi}}(1, \chi_0) \neq 0$ ([6, Chapter IV Proposition 5.7]).

Lemma 2.4. *Let $A \subsetneq B$ be finite abelian groups, $b \in B - A$ and χ be a character of A . Let m be the order of the coset bA in the quotient group B/A . Then we can extend χ to a character ψ of B such that $\psi(b)$ is any m^{th} root of $\chi(b^m)$.*

Proof. It suffices to prove the case $B = \langle A, b \rangle$. Let ζ be any m^{th} root of $\chi(b^m)$. Define a map

$$\begin{aligned} \psi : \langle A, b \rangle &\longrightarrow \mathbb{C}^* \\ ab^k &\mapsto \chi(a)\zeta^k \quad (a \in A). \end{aligned}$$

Using the fact $\zeta^m = \chi(b^m)$ one can readily show that ψ is a well-defined character of $\langle A, b \rangle$ which extends χ and also satisfies $\psi(b) = \zeta$. \square

Lemma 2.5. *Let K be an imaginary quadratic field and $\mathfrak{f} = \prod_{k=1}^n \mathfrak{p}_k^{e_k}$ be a nontrivial ideal of K . Let L be a finite abelian extension of K such that $K \subsetneq L \subseteq K_{\mathfrak{f}}$. For an intermediate field F between K and $K_{\mathfrak{f}}$ we denote by $\text{Cl}(K_{\mathfrak{f}}/F)$ the subgroup of $\text{Cl}(\mathfrak{f})$ corresponding to $\text{Gal}(K_{\mathfrak{f}}/F)$ via the Artin map. Let*

$$\begin{aligned}\widehat{\varepsilon}_k &= \# \text{Ker}(\text{the natural projection } \widehat{\rho}_k : \pi_{\mathfrak{f}}(\mathcal{O}_K)^* / \pi_{\mathfrak{f}}(\mathcal{O}_K^*) \rightarrow \pi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}(\mathcal{O}_K)^* / \pi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}(\mathcal{O}_K^*)), \\ \varepsilon_k &= \# \text{Ker}(\text{the natural projection } \rho_k : \pi_{\mathfrak{f}}(\mathcal{O}_K)^* / \pi_{\mathfrak{f}}(\mathcal{O}_K^*) \rightarrow \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* / \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K^*))\end{aligned}$$

for each $k = 1, \dots, n$. Assume that

$$\begin{aligned}\text{for each } k = 1, \dots, n \text{ there is an odd prime } \nu_k \text{ such that} \\ \nu_k \nmid \varepsilon_k \text{ and } \text{ord}_{\nu_k}(\widehat{\varepsilon}_k) > \text{ord}_{\nu_k}(\# \text{Cl}(K_{\mathfrak{f}}/L)).\end{aligned}\tag{2.3}$$

If D is a class in $\text{Cl}(\mathfrak{f}) - \text{Cl}(K_{\mathfrak{f}}/L)$, then there exists a character χ of $\text{Cl}(\mathfrak{f})$ such that

$$\chi|_{\text{Cl}(K_{\mathfrak{f}}/L)} = 1, \quad \chi(D) \neq 1 \text{ and } \mathfrak{p}_k | \mathfrak{f}_{\chi} \quad (k = 1, \dots, n).\tag{2.4}$$

Proof. Since $D \in \text{Cl}(\mathfrak{f}) - \text{Cl}(K_{\mathfrak{f}}/L)$, there is a character χ of $\text{Cl}(\mathfrak{f})$ such that

$$\chi|_{\text{Cl}(K_{\mathfrak{f}}/L)} = 1 \text{ and } \chi(D) \neq 1$$

by Lemma 2.4. Let $\widetilde{\chi}_k$ ($k = 1, \dots, n$) be the character of $\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*$ induced from χ as in Lemma 2.1.

Suppose $\widetilde{\chi}_k = 1$ for some k . Let ν_k be a prime number in the assumption (2.3) and S be a Sylow ν_k -subgroup of $\Phi_{\mathfrak{f}}(\text{Ker}(\widehat{\rho}_k))$. Then $\text{Cl}(K_{\mathfrak{f}}/L)$ does not contain S by (2.3). Hence we can take an element C in $S - \text{Cl}(K_{\mathfrak{f}}/L)$ whose order is a power of ν_k . Now we extend the trivial character of $\text{Cl}(K_{\mathfrak{f}}/L)$ to a character ψ' of $\text{Cl}(\mathfrak{f})$ so that $\psi'(C) = \zeta_{\nu_k} = e^{2\pi i/\nu_k}$ by Lemma 2.4, because the order of the coset $C\text{Cl}(K_{\mathfrak{f}}/L)$ in the quotient group $\text{Cl}(\mathfrak{f})/\text{Cl}(K_{\mathfrak{f}}/L)$ is also a power of ν_k . Define a character ψ of $\text{Cl}(\mathfrak{f})$ by

$$\psi = \begin{cases} \psi'^{\varepsilon_k} & \text{if } \chi(D)\psi'^{\varepsilon_k}(D) \neq 1 \\ \psi'^{2\varepsilon_k} & \text{otherwise.} \end{cases}$$

We then achieve $(\chi\psi)|_{\text{Cl}(K_{\mathfrak{f}}/L)} = 1$ and $(\chi\psi)(D) = \chi(D)\psi(D) \neq 1$. Furthermore, since $(\iota \circ \iota_{\ell}(\pi_{\mathfrak{p}_{\ell}^{e_{\ell}}}(\mathcal{O}_K)^*))\pi_{\mathfrak{f}}(\mathcal{O}_K^*)/\pi_{\mathfrak{f}}(\mathcal{O}_K^*)$ is a subgroup of $\text{Ker}(\rho_k)$ for $\ell \neq k$ (see the diagram (2.5) below), we derive that

$$\begin{aligned}\widetilde{\psi}_{\ell}(\pi_{\mathfrak{p}_{\ell}^{e_{\ell}}}(\mathcal{O}_K)^*) &= \psi \circ \widetilde{\Phi}_{\mathfrak{f}} \circ \iota \circ \iota_{\ell}(\pi_{\mathfrak{p}_{\ell}^{e_{\ell}}}(\mathcal{O}_K)^*) \quad \text{by the definition of } \widetilde{\psi}_{\ell} \text{ in Lemma 2.1} \\ &\subseteq \psi(\Phi_{\mathfrak{f}}(\text{Ker}(\rho_k))) \\ &= \psi'^{\varepsilon_k}(\Phi_{\mathfrak{f}}(\text{Ker}(\rho_k))) \text{ or } \psi'^{2\varepsilon_k}(\Phi_{\mathfrak{f}}(\text{Ker}(\rho_k))) = 1,\end{aligned}$$

which yields $\widetilde{\psi}_{\ell} = 1$ and $(\widetilde{\chi\psi})_{\ell} = \widetilde{\chi}_{\ell}\widetilde{\psi}_{\ell} = \widetilde{\chi}_{\ell}$ for $\ell \neq k$. On the other hand, since $C \in \Phi_{\mathfrak{f}}(\text{Ker}(\widehat{\rho}_k)) \subseteq \text{Im}(\Phi_{\mathfrak{f}})$, we can take an element c of $\pi_{\mathfrak{f}}(\mathcal{O}_K)^*$ so that $\widetilde{\Phi}_{\mathfrak{f}}(c) = C$. Thus we get

$$\widetilde{\psi}(c) = \psi \circ \widetilde{\Phi}_{\mathfrak{f}}(c) = \psi(C) = (\psi'^{\varepsilon_k}(C) \text{ or } \psi'^{2\varepsilon_k}(C)) = (\zeta_{\nu_k}^{\varepsilon_k} \text{ or } \zeta_{\nu_k}^{2\varepsilon_k}) \neq 1,$$

which shows $\widetilde{\psi} \neq 1$. Hence $\widetilde{\psi}_k \neq 1$ by the fact $\widetilde{\psi}_{\ell} = 1$ for $\ell \neq k$ and Lemma 2.1(ii). Therefore we obtain $(\widetilde{\chi\psi})_k = \widetilde{\chi}_k\widetilde{\psi}_k = \widetilde{\psi}_k \neq 1$.

Now, we replace χ by $\chi\psi$ and repeat the above process for finitely many ℓ ($\neq k$) such that $\tilde{\chi}_\ell = 1$. After this procedure we finally establish a character χ of $\text{Cl}(\mathfrak{f})$ which satisfies

$$\chi|_{\text{Cl}(K_{\mathfrak{f}}/L)} = 1, \quad \chi(D) \neq 1 \text{ and } \tilde{\chi}_k \neq 1 \quad (k = 1, \dots, n).$$

We derive by Lemma 2.1 that $\mathfrak{p}_k | \mathfrak{f}_\chi$ for all $k = 1, \dots, n$. This proves the lemma. \square

Remark 2.6. From the commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_{\mathfrak{f}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}}(\mathcal{O}_K^*) & \xrightarrow{\Phi_{\mathfrak{f}}} & \text{Cl}(\mathfrak{f}) & \longrightarrow & \text{Cl}(\mathcal{O}_K) & \longrightarrow & 1 \\ & & \downarrow \widehat{\rho}_k & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \pi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}(\mathcal{O}_K^*) & \xrightarrow{\Phi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}} & \text{Cl}(\mathfrak{f}\mathfrak{p}_k^{-e_k}) & \longrightarrow & \text{Cl}(\mathcal{O}_K) & \longrightarrow & 1 \end{array}$$

where vertical maps are natural projections, one can readily obtain

$$\text{Cl}(\mathfrak{f})/\Phi_{\mathfrak{f}}(\text{Ker}(\widehat{\rho}_k)) \simeq \text{Cl}(\mathfrak{f}\mathfrak{p}_k^{-e_k}) \simeq \text{Cl}(\mathfrak{f})/\text{Cl}(K_{\mathfrak{f}}/K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}).$$

Hence we have

$$\widehat{\varepsilon}_k = \# \text{Ker}(\widehat{\rho}_k) = \# \Phi_{\mathfrak{f}}(\text{Ker}(\widehat{\rho}_k)) = [K_{\mathfrak{f}} : K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}] = \varphi(\mathfrak{p}_k^{e_k})\omega(\mathfrak{f})/\omega(\mathfrak{f}\mathfrak{p}_k^{-e_k})$$

by using Lemma 3.7(ii), which will be used in the next section. Similarly, again from the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_{\mathfrak{f}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}}(\mathcal{O}_K^*) & \xrightarrow{\Phi_{\mathfrak{f}}} & \text{Cl}(\mathfrak{f}) & \longrightarrow & \text{Cl}(\mathcal{O}_K) & \longrightarrow & 1 \\ & & \downarrow \wr & & \downarrow & & \downarrow & & \\ \prod_{\ell=1}^n \pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^*/\{\prod_{\ell=1}^n \pi_{\mathfrak{p}_\ell^{e_\ell}}(x) : x \in \mathcal{O}_K^*\} & & \downarrow \rho_k & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*/\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K^*) & \xrightarrow{\Phi_{\mathfrak{p}_k^{e_k}}} & \text{Cl}(\mathfrak{p}_k^{e_k}) & \longrightarrow & \text{Cl}(\mathcal{O}_K) & \longrightarrow & 1 \end{array} \quad (2.5)$$

we come up with

$$\varepsilon_k = \# \text{Ker}(\rho_k) = \# \Phi_{\mathfrak{f}}(\text{Ker}(\rho_k)) = [K_{\mathfrak{f}} : K_{\mathfrak{p}_k^{e_k}}] = \frac{\prod_{\ell=1}^n \varphi(\mathfrak{p}_\ell^{e_\ell})\omega(\mathfrak{f})}{\varphi(\mathfrak{p}_k^{e_k})\omega(\mathfrak{p}_k^{e_k})}.$$

Theorem 2.7. *Let L be a field in Lemma 2.5 which satisfies the assumption (2.3). Then the singular value*

$$\varepsilon = \mathbf{N}_{K_{\mathfrak{f}}/L}(g_{\mathfrak{f}}(C_0))$$

generates L over K .

Proof. Let $F = K(\varepsilon)$ as a subfield of L . Suppose that F is properly contained in L . Then for a class D in $\text{Cl}(K_{\mathfrak{f}}/F) - \text{Cl}(K_{\mathfrak{f}}/L)$ we can find a character χ of $\text{Cl}(\mathfrak{f})$ satisfying the conditions

(2.4) in Lemma 2.5. Since the Euler factor of χ is 1 by the condition $\mathfrak{p}_k | \mathfrak{f}_\chi$ for all k , the value $S_{\mathfrak{f}}(\bar{\chi}, g_{\mathfrak{f}})$ does not vanish by Proposition 2.2 and Remark 2.3(ii). On the other hand,

$$\begin{aligned}
S_{\mathfrak{f}}(\bar{\chi}, g_{\mathfrak{f}}) &= \sum_{\substack{C_1 \in \text{Cl}(\mathfrak{f}) \\ C_1 \bmod \text{Cl}(K_{\mathfrak{f}}/F)}} \sum_{\substack{C_2 \in \text{Cl}(K_{\mathfrak{f}}/F) \\ C_2 \bmod \text{Cl}(K_{\mathfrak{f}}/L)}} \sum_{C_3 \in \text{Cl}(K_{\mathfrak{f}}/L)} \bar{\chi}(C_1 C_2 C_3) \log |g_{\mathfrak{f}}(C_1 C_2 C_3)| \\
&= \sum_{C_1} \bar{\chi}(C_1) \sum_{C_2} \bar{\chi}(C_2) \sum_{C_3} \log |g_{\mathfrak{f}}(C_0)^{\sigma(C_1)\sigma(C_2)\sigma(C_3)}| \quad \text{by } \chi|_{\text{Cl}(K_{\mathfrak{f}}/L)} = 1 \text{ and (2.2)} \\
&= \sum_{C_1} \bar{\chi}(C_1) \sum_{C_2} \bar{\chi}(C_2) \log |\varepsilon^{\sigma(C_1)\sigma(C_2)}| \\
&= \sum_{C_1} \bar{\chi}(C_1) \left(\sum_{C_2} \bar{\chi}(C_2) \right) \log |\varepsilon^{\sigma(C_1)}| \quad \text{by the fact } \varepsilon \in F \\
&= 0 \quad \text{because } \chi(D) \neq 1 \text{ implies } \chi|_{\text{Cl}(K_{\mathfrak{f}}/F)} \neq 1,
\end{aligned}$$

which gives a contradiction. Therefore $L = F$, as desired. \square

Remark 2.8. Observe that any nonzero power of ε generates L over K , too.

3. ACTIONS OF GALOIS GROUPS

In this section we shall determine Galois groups of ray class fields over ring class fields by Shimura's reciprocity law.

For an integer $N (\geq 1)$ let $\zeta_N = e^{2\pi i/N}$ and $\Gamma(N) = \{\gamma \in \text{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\}$. Furthermore, we let \mathcal{F}_N be the field of modular functions for $\Gamma(N)$ whose Fourier coefficients lie in $\mathbb{Q}(\zeta_N)$.

Proposition 3.1. \mathcal{F}_N is a Galois extension of $\mathcal{F}_1 = \mathbb{Q}(j(\tau))$ whose Galois group is isomorphic to

$$\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} = G_N \cdot \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} = \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \cdot G_N,$$

where $G_N = \{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} : d \in (\mathbb{Z}/N\mathbb{Z})^* \}$. Here, the matrix $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \in G_N$ acts on $\sum_{n>-\infty} c_n q^{n/N} \in \mathcal{F}_N$ by

$$\sum_{n>-\infty} c_n q^{n/N} \mapsto \sum_{n>-\infty} c_n^{\sigma_d} q^{n/N},$$

where σ_d is the automorphism of $\mathbb{Q}(\zeta_N)$ induced by $\zeta_N \mapsto \zeta_N^d$. And, for an element $\gamma \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ let $\gamma' \in \text{SL}_2(\mathbb{Z})$ be a preimage of γ via the natural surjection $\text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$. Then γ acts on $h \in \mathcal{F}_N$ by composition

$$h \mapsto h \circ \gamma'$$

as a fractional linear transformation.

Proof. See [12, Chapter 6 Theorem 3]. \square

Proposition 3.2. Let N be a positive integer.

- (i) The fixed field of \mathcal{F}_N by $\Gamma_0(N)$ is the field $\mathbb{Q}(j(\tau), j(N\tau), \zeta_N)$.
- (ii) $j(N\tau)$ has rational Fourier coefficients.
- (iii) $\Delta(N\tau)/\Delta(\tau)$ belongs to \mathcal{F}_N and has rational Fourier coefficients.

Proof. (i) See [12, Chapter 6 Theorem 7].

(ii) See [12, Chapter 4 §1].

(iii) See [12, Chapter 11 Theorem 4]. \square

We need some transformation formulas of Siegel functions to apply the above proposition.

Proposition 3.3. *Let $(r_1, r_2) \in (1/N)\mathbb{Z}^2 - \mathbb{Z}^2$ for $N \geq 2$.*

(i) $g_{(r_1, r_2)}(\tau)^{12N}$ satisfies

$$g_{(r_1, r_2)}(\tau)^{12N} = g_{(-r_1, -r_2)}(\tau)^{12N} = g_{(\langle r_1 \rangle, \langle r_2 \rangle)}(\tau)^{12N},$$

where $\langle X \rangle$ is the fractional part of $X \in \mathbb{R}$ such that $0 \leq \langle X \rangle < 1$.

(ii) $g_{(r_1, r_2)}(\tau)^{12N}$ belongs to \mathcal{F}_N , and $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ ($\simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$) acts on the function by

$$(g_{(r_1, r_2)}(\tau)^{12N})^\alpha = g_{(r_1, r_2)\alpha}(\tau)^{12N}.$$

(iii) $g_{(r_1, r_2)}(\tau)$ is integral over $\mathbb{Z}[j(\tau)]$.

Proof. (i) See [8, Proposition 2.4(1), (3)].

(ii) See [10, Chapter 2 Proposition 1.3].

(iii) See [8, §3]. \square

Let K be an imaginary quadratic field of discriminant d_K , and define

$$\theta = \begin{cases} \sqrt{d_K}/2 & \text{for } d_K \equiv 0 \pmod{4} \\ (-1 + \sqrt{d_K})/2 & \text{for } d_K \equiv 1 \pmod{4}, \end{cases} \quad (3.1)$$

from which we get $\mathcal{O}_K = \mathbb{Z}[\theta]$. We see from the main theorem of the theory of complex multiplication that for every positive integer N ,

$$K_{(N)} = K\mathcal{F}_N(\theta) = K(h(\theta)) : h \in \mathcal{F}_N \text{ is defined and finite at } \theta$$

([12, Chapter 10 Corollary to Theorem 2]).

Let

$$\min(\theta, \mathbb{Q}) = X^2 + B_\theta X + C_\theta = \begin{cases} X^2 - d_K/4 & \text{if } d_K \equiv 0 \pmod{4} \\ X^2 + X + (1 - d_K)/4 & \text{if } d_K \equiv 1 \pmod{4}. \end{cases}$$

For every positive integer N , we define the matrix group

$$W_{N, \theta} = \left\{ \begin{pmatrix} t - B_\theta s & -C_\theta s \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : t, s \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

Due to Steinhagen we have the following explicit description of Shimura's reciprocity law ([15, Theorem 6.31 and Proposition 6.34]), which relates the class field theory to the theory of modular functions.

Proposition 3.4. *For each positive integer N , the matrix group $W_{N, \theta}$ gives rise to the surjection*

$$\begin{aligned} W_{N, \theta} &\longrightarrow \mathrm{Gal}(K_{(N)}/H) \\ \alpha &\mapsto (h(\theta) \mapsto h^\alpha(\theta)) : h \in \mathcal{F}_N \text{ is defined and finite at } \theta, \end{aligned} \quad (3.2)$$

whose kernel is

$$\begin{cases} \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\} & \text{if } K = \mathbb{Q}(\sqrt{-1}) \\ \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right\} & \text{if } K = \mathbb{Q}(\sqrt{-3}) \\ \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} & \text{otherwise.} \end{cases}$$

Proof. See [16, §3]. \square

The ring class field $H_{\mathcal{O}}$ of the order \mathcal{O} of conductor $N (\geq 1)$ in K is by the definition a finite abelian extension of K whose Galois group is isomorphic to $I_K(N\mathcal{O}_K)/P_{K,\mathbb{Z}}(N\mathcal{O}_K)$ via the Artin map, where $P_{K,\mathbb{Z}}(N\mathcal{O}_K)$ is the subgroup of $P_K(N\mathcal{O}_K)$ generated by principal ideals $\alpha\mathcal{O}_K$ with $\alpha \equiv a \pmod{N\mathcal{O}_K}$ for some integer a prime to N . Then, $H_{\mathcal{O}}$ is contained in the ray class field $K_{(N)}$.

Proposition 3.5. *Let K be an imaginary quadratic field and θ be as in (3.1). Let \mathcal{O} be the order of conductor $N (\geq 1)$ in K .*

- (i) $j(\mathcal{O}) = j(N\theta)$ is an algebraic integer which generates $H_{\mathcal{O}}$ over K .
- (ii) $\Delta(N\theta)/\Delta(\theta)$ is a real algebraic number lying in $H_{\mathcal{O}}$.

Proof. (i) See [12, Chapter 5 Theorem 4 and Chapter 10 Theorem 5].

(ii) See [12, Chapter 12 Corollary to Theorem 1]. \square

Lemma 3.6. *Let K be an imaginary quadratic field and θ be as in (3.1). Let N be a positive integer. Then, $\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \in W_{N,\theta}$ fixes $j(N\theta)$.*

Proof. Decompose $\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \in W_{N,\theta}$ into $\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & t^2 \end{pmatrix} \cdot \alpha \in G_N \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ as in Proposition 3.1, and let α' be a preimage of α via the natural surjection $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$. Then, α' belongs to $\Gamma_0(N)$. We then obtain from Propositions 3.1 and 3.4 that

$$\begin{aligned} j(N\theta)^{\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}} &= j(N\tau)^{\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}}(\theta) = j(N\tau)^{\begin{pmatrix} 1 & 0 \\ 0 & t^2 \end{pmatrix}\alpha}(\theta) \\ &= j(N\tau)^{\alpha}(\theta) \quad \text{by Proposition 3.2(ii)} \\ &= j(N\tau) \circ \alpha'(\theta) \\ &= j(N\theta) \quad \text{by the fact } \alpha' \in \Gamma_0(N) \text{ and Proposition 3.2(i).} \end{aligned}$$

This proves the lemma. \square

Lemma 3.7. *Let K be an imaginary quadratic field of discriminant d_K . We have the following degree formulas:*

- (i) *If \mathcal{O} is the order of conductor $N (\geq 1)$ in K , then*

$$[H_{\mathcal{O}} : K] = \frac{h_K N}{(\mathcal{O}_K^* : \mathcal{O}^*)} \prod_{p|N} \left(1 - \left(\frac{d_K}{p} \right) \frac{1}{p} \right),$$

where h_K is the class number of K and (d_K/p) is the Kronecker symbol.

(ii) If \mathfrak{f} is a nonzero integral ideal of K , then

$$[K_{\mathfrak{f}} : K] = h_K \varphi(\mathfrak{f}) \omega(\mathfrak{f}) / \omega_K,$$

where φ is the Euler function for ideals, namely

$$\varphi(\mathfrak{p}^n) = (\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p}) - 1) \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p})^{n-1}$$

for a power of prime ideal \mathfrak{p} (and we set $\varphi(\mathcal{O}_K) = 1$).

Proof. (i) See [12, Chapter 8 Theorem 7].

(ii) See [11, Chapter VI Theorem 1]. \square

Proposition 3.8. *Let \mathcal{O} be the order of conductor N (≥ 1) in an imaginary quadratic field K . The map in (3.2) induces an isomorphism*

$$\left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} : t \in (\mathbb{Z}/N\mathbb{Z})^* \right\} / \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \xrightarrow{\sim} \text{Gal}(K_{(N)}/H_{\mathcal{O}}).$$

Proof. If $N = 1$, then it is obvious. So, let $N \geq 2$. Observe first that the above map is well-defined and injective by Proposition 3.4 and Lemma 3.6. Let $N = \prod_{a=1}^A p_a^{u_a} \prod_{b=1}^B q_b^{v_b} \prod_{c=1}^C r_c^{w_c}$ be the prime factorization of N , where each p_a (respectively, q_b and r_c) splits (respectively, is inert and ramified) in K/\mathbb{Q} . (We understand \prod_1^0 as 1.) Note that

$$(d_K/p_a) = 1, (d_K/q_b) = -1, (d_K/r_c) = 0, \quad (3.3)$$

and we have the prime ideal factorization $N\mathcal{O}_K = \prod_{a=1}^A (\mathfrak{p}_a \bar{\mathfrak{p}}_a)^{u_a} \prod_{b=1}^B \mathfrak{q}_b^{v_b} \prod_{c=1}^C \mathfrak{r}_c^{2w_c}$ with

$$\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p}_a) = \mathbf{N}_{K/\mathbb{Q}}(\bar{\mathfrak{p}}_a) = p_a, \quad \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{q}_b) = q_b^2, \quad \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{r}_c) = r_c. \quad (3.4)$$

We derive by Lemma 3.7 that

$$\begin{aligned} \# \text{Gal}(K_{(N)}/H_{\mathcal{O}}) &= [K_{(N)} : H_{\mathcal{O}}] = \frac{[K_{(N)} : K]}{[H_{\mathcal{O}} : K]} \\ &= \frac{\varphi(N\mathcal{O}_K) \omega(N\mathcal{O}_K)}{2N \prod_{p|N} (1 - (\frac{d_K}{p}) \frac{1}{p})} \quad \text{by the facts } \omega_K = \# \mathcal{O}_K^* \text{ and } \mathcal{O}^* = \{\pm 1\} \\ &= \frac{\omega(N\mathcal{O}_K) \prod_{a=1}^A ((p_a - 1) p_a^{u_a - 1})^2 \prod_{b=1}^B (q_b^2 - 1) q_b^{2(v_b - 1)} \prod_{c=1}^C (r_c - 1) r_c^{2w_c - 1}}{2 \prod_{a=1}^A p_a^{u_a - 1} (p_a - 1) \prod_{b=1}^B q_b^{v_b - 1} (q_b + 1) \prod_{c=1}^C r_c^{w_c}} \\ &\quad \text{by (3.3) and (3.4)} \\ &= \frac{\omega(N\mathcal{O}_K)}{2} \prod_{a=1}^A (p_a - 1) p_a^{u_a - 1} \prod_{b=1}^B (q_b - 1) q_b^{v_b - 1} \prod_{c=1}^C (r_c - 1) r_c^{w_c - 1} \\ &= \frac{\omega(N\mathcal{O}_K)}{2} \phi(N) \quad \text{where } \phi \text{ is the Euler function for integers} \\ &= \# \left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} : t \in (\mathbb{Z}/N\mathbb{Z})^* \right\} / \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}. \end{aligned}$$

This concludes the proposition. \square

Remark 3.9. Lemma 3.6 and Proposition 3.8 have been given in [9, Lemma 5.2 and Proposition 5.3] without much explanation. For completeness we present their proof in detail.

4. RING CLASS INVARIANTS

We shall make use of Theorem 2.7 to construct primitive generators of ring class fields as the singular values of certain Δ -quotients.

Lemma 4.1. *For a positive integer N , we have the relation*

$$\prod_{t=1}^{N-1} g_{(0,t/N)}(\tau)^{12} = N^{12} \Delta(N\tau) / \Delta(\tau),$$

where the left hand side is regarded as 1 when $N = 1$.

Proof. For $N \geq 2$ we find that

$$\begin{aligned} & \prod_{t=1}^{N-1} g_{(0,t/N)}(\tau)^{12} \\ &= \prod_{t=1}^{N-1} \left(-q^{1/12} \zeta_{2N}^{-t} (1 - \zeta_N^t) \prod_{n=1}^{\infty} (1 - q^n \zeta_N^t) (1 - q^n \zeta_N^{-t}) \right)^{12} \quad \text{by the definition (1.1)} \\ &= q^{N-1} N^{12} \prod_{n=1}^{\infty} ((1 - q^{Nn}) / (1 - q^n))^{24} \quad \text{by the identity } \prod_{t=1}^{N-1} (1 - \zeta_N^t X) = (1 - X^N) / (1 - X) \\ &= N^{12} \Delta(N\tau) / \Delta(\tau) \quad \text{by the definition (1.2).} \end{aligned}$$

□

We are ready to prove our first main theorem.

Theorem 4.2. *Let K be an imaginary quadratic field and θ be as in (3.1). Let \mathcal{O} be the order of conductor $N = \prod_{k=1}^n p_k^{e_k}$ (≥ 2) in K . Set*

$$N_S = \begin{cases} \prod_{k \in S} p_k & \text{if } S \text{ is a nonempty subset of } \{1, 2, \dots, n\} \\ 1 & \text{if } S = \emptyset. \end{cases}$$

If $\mathfrak{f} = N\mathcal{O}_K$ satisfies the assumption (2.3) in Lemma 2.5, then the singular value

$$\begin{cases} p_1^{12} \Delta(p_1^{e_1} \theta) / \Delta(p_1^{e_1-1} \theta) & \text{if } n = 1 \\ \prod_{S \subseteq \{1, 2, \dots, n\}} \Delta((N/N_S) \theta)^{(-1)^{\#S}} & \text{if } n \geq 2 \end{cases} \quad (4.1)$$

generates $H_{\mathcal{O}}$ over K as a real algebraic integer.

Proof. If $\mathfrak{f} = N\mathcal{O}_K$, then $g_{\mathfrak{f}}(C_0) = g_{(0,1/N)}(\theta)^{12N}$ by the definition. We get that

$$\begin{aligned}
& \begin{cases} \mathbf{N}_{K_{\mathfrak{f}}/H_{\mathcal{O}}}(g_{\mathfrak{f}}(C_0)) & \text{if } N = 2 \\ \mathbf{N}_{K_{\mathfrak{f}}/H_{\mathcal{O}}}(g_{\mathfrak{f}}(C_0))^2 & \text{if } N \geq 3 \end{cases} \\
&= \prod_{\substack{1 \leq t \leq N-1 \\ \gcd(t,N)=1}} (g_{(0,1/N)}(\theta)^{12N})^{\binom{t}{0} \binom{0}{t}} \quad \text{by Proposition 3.8} \\
&= \prod_{\substack{1 \leq t \leq N-1 \\ \gcd(t,N)=1}} (g_{(0,1/N)}(\tau)^{12N})^{\binom{t}{0} \binom{0}{t}}(\theta) \quad \text{by Proposition 3.4} \\
&= \prod_{\substack{1 \leq t \leq N-1 \\ \gcd(t,N)=1}} g_{(0,t/N)}(\theta)^{12N} \quad \text{by Proposition 3.3(ii)} \\
&= \prod_{S \subseteq \{1,2,\dots,n\}} \left(\prod_{1 \leq t \leq N-1, N_S | t} g_{(0,t/N)}(\theta)^{12} \right)^{N(-1)^{\#S}} \quad \text{by inclusion-exclusion principle} \\
&= \prod_{S \subseteq \{1,2,\dots,n\}} \left(\prod_{w=1}^{(N/N_S)-1} g_{(0,N_S w/N)}(\theta)^{12} \right)^{N(-1)^{\#S}} \quad \text{by setting } t = N_S w \\
&= \prod_{S \subseteq \{1,2,\dots,n\}} ((N/N_S)^{12} \Delta((N/N_S)\theta)/\Delta(\theta))^{N(-1)^{\#S}} \quad \text{by Lemma 4.1,} \tag{4.2}
\end{aligned}$$

which is a generator of $H_{\mathcal{O}}$ over K by Theorem 2.7 and Remark 2.8. On the other hand, the value $\mathbf{N}_{K_{\mathfrak{f}}/H_{\mathcal{O}}}(g_{\mathfrak{f}}(C_0))$ is an algebraic integer by Propositions 3.3(iii) and 3.5(i). Furthermore, each factor $\Delta((N/N_S)\theta)/\Delta(\theta)$ appeared in (4.2) belongs to the ring class field of the order of conductor N/N_S in K as a real algebraic number by Proposition 3.5(ii). Therefore the value in (4.2) without N^{th} power generates $H_{\mathcal{O}}$ over K as an algebraic integer. We further observe that

$$\begin{aligned}
& \prod_{S \subseteq \{1,2,\dots,n\}} ((N/N_S)^{12} \Delta((N/N_S)\theta)/\Delta(\theta))^{(-1)^{\#S}} \\
&= (N^{12}/\Delta(\theta))^{\sum_{S \subseteq \{1,2,\dots,n\}} (-1)^{\#S}} \prod_{S \subseteq \{1,2,\dots,n\}} N_S^{-12(-1)^{\#S}} \prod_{S \subseteq \{1,2,\dots,n\}} \Delta((N/N_S)\theta)^{(-1)^{\#S}} \\
&= \begin{cases} (p_1^{12e_1}/\Delta(\theta))^{1-1} p_1^{12} \Delta(p_1^{e_1}\theta) \Delta(p_1^{e_1-1}\theta)^{-1} & \text{if } n = 1 \\ (N^{12}/\Delta(\theta))^{\sum_{k=0}^n \binom{n}{k} (-1)^k} \prod_{k=1}^n p_k^{-12 \sum_{\ell=1}^n \binom{n-1}{\ell-1} (-1)^{\ell}} & \text{if } n \geq 2 \end{cases} \\
&= \begin{cases} p_1^{12} \Delta(p_1^{e_1}\theta)/\Delta(p_1^{e_1-1}\theta) & \text{if } n = 1 \\ \prod_{S \subseteq \{1,2,\dots,n\}} \Delta((N/N_S)\theta)^{(-1)^{\#S}} & \text{if } n \geq 2. \end{cases}
\end{aligned}$$

This completes the proof. \square

Remark 4.3. Let \mathcal{O} be the order of conductor $N = \prod_{k=1}^n p_k^{e_k}$ (≥ 2) in an imaginary quadratic field K . Denote by r_k the ramification index of p_k in K/\mathbb{Q} for each $k = 1, \dots, n$. Assume first that

$$\text{each } p_k \text{ is an odd prime which is inert or ramified in } K/\mathbb{Q}. \quad (4.3)$$

Since $N\mathcal{O}_K = \prod_{k=1}^n \mathfrak{p}_k^{r_k e_k}$ with $\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p}_k) = p_k^{2/r_k}$, we have

$$\widehat{\varepsilon}_k = \begin{cases} (1/\omega_K)(p_1^{2/r_1} - 1)p_1^{2e_1-2/r_1} & \text{if } n = 1 \\ (p_k^{2/r_k} - 1)p_k^{2e_k-2/r_k} & \text{if } n \geq 2 \end{cases}, \quad \varepsilon_k = \frac{\prod_{\ell=1}^n (p_\ell^{2/r_\ell} - 1)p_\ell^{2e_\ell-2/r_\ell}}{(p_k^{2/r_k} - 1)p_k^{2e_k-2/r_k}} \quad (k = 1, \dots, n),$$

and $\# \text{Cl}(K_{(N)}/H_{\mathcal{O}}) = (1/2) \prod_{k=1}^n (p_k - 1)p_k^{e_k-1}$ by Proposition 3.8. Assume further that

$$e_k + 1 > 2/r_k \quad (k = 1, \dots, n) \text{ and } \begin{cases} \gcd(p_1, \omega_K) = 1 & \text{if } n = 1 \\ \gcd(\prod_{k=1}^n p_k, \prod_{k=1}^n (p_k^{2/r_k} - 1)) = 1 & \text{if } n \geq 2. \end{cases} \quad (4.4)$$

Then, since

$$p_k \nmid \varepsilon_k \text{ and } \text{ord}_{p_k}(\widehat{\varepsilon}_k) = 2e_k - 2/r_k > \text{ord}_{p_k}(\# \text{Cl}(K_{(N)}/H_{\mathcal{O}})) = e_k - 1 \quad (k = 1, \dots, n),$$

we can take $\nu_k = p_k$ as for the assumption (2.3) in Lemma 2.5. Therefore one can apply Theorem 4.2 under the assumptions (4.3) and (4.4).

Example 4.4. If $K = \mathbb{Q}(\sqrt{-7})$, then $\theta = (-1 + \sqrt{-7})/2$ and $h_K = 1$ ([4, Theorem 12.34]), in other words, $H = K$. Let \mathcal{O} be the order of conductor $N = 7$ in K . We get by Propositions 3.4 and 3.8 that

$$\begin{aligned} \text{Gal}(H_{\mathcal{O}}/K) &\simeq (W_{7,\theta}/\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\})/(\{(t \ 0) : t \in (\mathbb{Z}/7\mathbb{Z})^*\}/\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}) \\ &= \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 \\ 4 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 7 & 12 \\ -10 & -17 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \cdot \begin{pmatrix} -13 & -16 \\ 9 & 11 \end{pmatrix}, \\ &\quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -5 & -16 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -3 & -16 \\ 1 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \cdot \begin{pmatrix} -16 & -9 \\ 9 & 5 \end{pmatrix} \}. \end{aligned}$$

Note that we expressed elements of $\text{Gal}(H_{\mathcal{O}}/K)$ in the form of

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \text{ for some } d \in (\mathbb{Z}/7\mathbb{Z})^* \cdot \text{an element of } \text{SL}_2(\mathbb{Z}).$$

On the other hand, since 7 is ramified in K/\mathbb{Q} and $\omega_K = 2$, the assumptions (4.3) and (4.4) in Remark 4.3 (or, the assumption (5.22) in Remark 5.5) are satisfied. Hence the singular value $7^{12}\Delta(7\theta)/\Delta(\theta)$ generates $H_{\mathcal{O}}$ over K by Theorem 4.2 (or, Theorem 5.4). Furthermore, since the function $\Delta(7\tau)/\Delta(\tau)$ belongs to \mathcal{F}_7 and has rational Fourier coefficients by Proposition 3.2(iii), we obtain its minimal polynomial by Propositions 3.1 and 3.4 as

$$\begin{aligned} &\min(7^{12}\Delta(7\theta)/\Delta(\theta), K) \\ &= (X - (7^{12}\Delta(7\tau)/\Delta(\tau)) \circ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}(\theta))(X - (7^{12}\Delta(7\tau)/\Delta(\tau)) \circ \begin{pmatrix} -1 & -2 \\ 4 & 7 \end{pmatrix}(\theta)) \\ &\quad (X - (7^{12}\Delta(7\tau)/\Delta(\tau)) \circ \begin{pmatrix} 7 & 12 \\ -10 & -17 \end{pmatrix}(\theta))(X - (7^{12}\Delta(7\tau)/\Delta(\tau)) \circ \begin{pmatrix} -13 & -16 \\ 9 & 11 \end{pmatrix}(\theta)) \\ &\quad (X - (7^{12}\Delta(7\tau)/\Delta(\tau)) \circ \begin{pmatrix} -5 & -16 \\ 1 & 3 \end{pmatrix}(\theta))(X - (7^{12}\Delta(7\tau)/\Delta(\tau)) \circ \begin{pmatrix} -3 & -16 \\ 1 & 5 \end{pmatrix}(\theta)) \\ &\quad (X - (7^{12}\Delta(7\tau)/\Delta(\tau)) \circ \begin{pmatrix} -16 & -9 \\ 9 & 5 \end{pmatrix}(\theta)) \\ &= X^7 + 234857X^6 + 24694815621X^5 + 295908620105035X^4 + 943957383096939785X^3 \\ &\quad + 356807315211847521X^2 + 38973886319454982X - 117649. \end{aligned}$$

On the other hand, if we compare its coefficients with those of the minimal polynomial of the classical invariant $j(7\theta)$, we see in a similar fashion that the latter are much bigger than the former as follows:

$$\begin{aligned} & \min(j(7\theta), K) \\ = & X^7 + 18561099067532582351348250X^6 + 54379116263846797396254926859375X^5 \\ & + 344514398594838596665876837347342843995647646484375X^4 \\ & + 1009848457088842748174122781381460720529620832094970703125X^3 \\ & + 1480797351289795967859364968037513969226011238564633514404296875X^2 \\ & - 3972653601649066484326573605251406741304015473521796878814697265625X \\ & + 4791576562341747034548276661270093305105027267573103845119476318359375. \end{aligned}$$

Example 4.5. Let $K = \mathbb{Q}(\sqrt{-5})$ and \mathcal{O} be the order of conductor $N = 6 (= 2 \cdot 3)$ in K . One can readily check that $N\mathcal{O}_K$ satisfies neither the assumption (2.3) in Lemma 2.5 nor the assumption (5.22) in Remark 5.5. Even in this case, however, we will see that our method is still valid. Therefore, it is worth of studying how much further one can release from the assumption (2.3) in Lemma 2.5 (or, the assumption (5.22) in Remark 5.5).

Observe that $h_K = 2$ ([4, p.29]) and $[H_{\mathcal{O}} : K] = 8$ by Lemma 3.7(i). Since $h_K = 2$, there are two reduced positive definite binary quadratic forms of discriminant $d_K = -20$, namely

$$Q_1 = X^2 + 5Y^2 \text{ and } Q_2 = 2X^2 + 2XY + 3Y^2.$$

We associate to each Q_k ($k = 1, 2$) a matrix in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and a CM-point as follows:

$$\begin{cases} \beta_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \theta_1 = \sqrt{-5} & \text{for } Q_1 \\ \beta_2 = \begin{pmatrix} 1 & 5 \\ 3 & 2 \end{pmatrix}, \theta_2 = (-1 + \sqrt{-5})/2 & \text{for } Q_2. \end{cases}$$

Then we see from [16, §6] that

$$\text{Gal}(H/K) = \{(h(\theta) \mapsto h^{\beta_k}(\theta_k))|_H : k = 1, 2\},$$

where $h \in \mathcal{F}_N$ is defined and finite at $\theta = \sqrt{-5}$. Furthermore, it follows from Propositions 3.4 and 3.8 that

$$\text{Gal}(H_{\mathcal{O}}/H) \simeq \{\alpha_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \alpha_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \alpha_3 = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}, \alpha_4 = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}\}.$$

Hence we achieve that

$$\text{Gal}(H_{\mathcal{O}}/K) = \{(h(\theta) \mapsto h^{\alpha_{\ell}\beta_k}(\theta_k))|_{H_{\mathcal{O}}} : \ell = 1, \dots, 4, k = 1, 2\},$$

where $h \in \mathcal{F}_N$ is defined and finite at θ . The conjugates of $\Delta(6\theta)\Delta(\theta)/\Delta(2\theta)\Delta(3\theta)$ estimated according to Theorem 4.2 are

$$x_{\ell,k} = (\Delta(6\tau)\Delta(\tau)/\Delta(2\tau)\Delta(3\tau))^{\alpha_{\ell}\beta_k}(\theta_k) \quad (\ell = 1, \dots, 4, k = 1, 2)$$

possibly with some multiplicity. And, since the function $\Delta(6\tau)\Delta(\tau)/\Delta(2\tau)\Delta(3\tau) \in \mathcal{F}_N$ has rational Fourier coefficients, the action of each $\alpha_{\ell}\beta_k$ on it can be performed as in the previous

example. Thus the minimal polynomial of $\Delta(6\theta)\Delta(\theta)/\Delta(2\theta)\Delta(3\theta)$ becomes a divisor of

$$\begin{aligned} \prod_{\ell=1, \dots, 4, k=1, 2} (X - x_{\ell, k}) &= X^8 - 1304008X^7 + 16670918428X^6 + 30056736254344X^5 \\ &\quad + 23344024601638470X^4 + 7327603919934344X^3 \\ &\quad + 1949665164230428X^2 - 1597207512008X + 1. \end{aligned}$$

This polynomial is, however, irreducible and hence the singular value $\Delta(6\theta)\Delta(\theta)/\Delta(2\theta)\Delta(3\theta)$ should be a primitive generator of $H_{\mathcal{O}}$ over K .

5. ANOTHER APPROACH

We shall develop a different lemma which substitutes for Lemma 2.5, from which we are able to find more N 's in Theorem 4.2.

Throughout this section, we let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$, and θ be as in (3.1). Let \mathcal{O} be the order of conductor N (≥ 2) in K with

$$\mathfrak{f} = N\mathcal{O}_K = \prod_{k=1}^n \mathfrak{p}_k^{e_k}.$$

We use the same notations $\pi_{\mathfrak{f}}$, ι , ι_k , v_k , $\tilde{\Phi}_{\mathfrak{f}}$ as in §2. And, by $\text{Cl}(H_{\mathcal{O}}/K)$ we mean the quotient group of $\text{Cl}(\mathfrak{f})$ corresponding to $\text{Gal}(H_{\mathcal{O}}/K)$ via the Artin map, that is

$$\text{Cl}(H_{\mathcal{O}}/K) = \text{Cl}(\mathfrak{f})/\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}}). \quad (5.1)$$

We further let $\text{Cl}(H_{\mathcal{O}}/H)$ stand for the subgroup of $\text{Cl}(H_{\mathcal{O}}/K)$ corresponding to $\text{Gal}(H_{\mathcal{O}}/H)$.

Setting

$$\check{\Psi}_{\mathfrak{f}} = (\text{Cl}(\mathfrak{f}) \rightarrow \text{Cl}(H_{\mathcal{O}}/K)) \circ \tilde{\Phi}_{\mathfrak{f}} : \pi_{\mathfrak{f}}(\mathcal{O}_K)^* \longrightarrow \text{Cl}(H_{\mathcal{O}}/K), \quad (5.2)$$

we obtain from the exact sequence (2.1) and Galois theory another exact sequence

$$1 \longrightarrow \pi_{\mathfrak{f}}(\mathcal{O}_K)^*/\text{Ker}(\check{\Psi}_{\mathfrak{f}}) \longrightarrow \text{Cl}(H_{\mathcal{O}}/K) \longrightarrow \text{Cl}(\mathcal{O}_K) \longrightarrow 1 \quad (5.3)$$

with

$$\check{\Psi}_{\mathfrak{f}}(\pi_{\mathfrak{f}}(\mathcal{O}_K)^*) = \text{Cl}(H_{\mathcal{O}}/H). \quad (5.4)$$

We know by the fact $\omega_K = 2$ and Lemma 3.7 that

$$\#\pi_{\mathfrak{f}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}}(\mathbb{Z})^* = \varphi(\mathfrak{f})/\phi(N) \text{ and } [H_{\mathcal{O}} : H] = \varphi(\mathfrak{f})/\phi(N).$$

On the other hand, since $\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}}) = P_{K, \mathbb{Z}}(\mathfrak{f})/P_{K, 1}(\mathfrak{f})$ by the definition of $H_{\mathcal{O}}$, we get $\pi_{\mathfrak{f}}(\mathbb{Z})^* \subseteq \text{Ker}(\check{\Psi}_{\mathfrak{f}})$; hence we achieve

$$\text{Ker}(\check{\Psi}_{\mathfrak{f}}) = \pi_{\mathfrak{f}}(\mathbb{Z})^*. \quad (5.5)$$

Lemma 5.1. *Let G be a finite abelian group and H be a subgroup of G . There is a canonical isomorphism between character groups*

$$\begin{aligned} \{\text{characters of } G \text{ which are trivial on } H\} &\longrightarrow \{\text{characters of } G/H\} \\ \chi &\mapsto (gH \mapsto \chi(g) : g \in G). \end{aligned} \quad (5.6)$$

Proof. One can readily check that the map in (5.6) is a well-defined injection. For surjectivity, let ψ be a character of G/H . Then the character

$$\chi = \psi \circ (G \rightarrow G/H)$$

of G maps to ψ via the map in (5.6), which claims the surjectivity. \square

Thus we have a canonical isomorphism

$$\{\text{characters of } \text{Cl}(\mathfrak{f}) \text{ which are trivial on } \text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})\} \longrightarrow \{\text{characters of } \text{Cl}(H_{\mathcal{O}}/K)\} \quad (5.7)$$

by Lemma 5.1 and definition (5.1). For any character ψ of $\text{Cl}(H_{\mathcal{O}}/K)$ we define

$$\check{\psi} = \psi \circ \check{\Psi}_{\mathfrak{f}} \text{ and } \check{\psi}_k = \check{\psi} \circ \iota \circ \iota_k \quad (k = 1, \dots, n).$$

If χ maps to ψ via the map in (5.7), then we derive

$$\begin{aligned} \tilde{\chi} &= \chi \circ \tilde{\Phi}_{\mathfrak{f}} = \psi \circ (\text{Cl}(\mathfrak{f}) \rightarrow \text{Cl}(H_{\mathcal{O}}/K)) \circ \tilde{\Phi}_{\mathfrak{f}} \quad \text{by the proof of Lemma 5.1} \\ &= \psi \circ \check{\Psi}_{\mathfrak{f}} = \check{\psi} \quad \text{by definition (5.2),} \end{aligned}$$

from which it follows that

$$\tilde{\chi}_k = \check{\psi}_k \quad (k = 1, \dots, n).$$

Lemma 5.2. *Let*

$$\begin{aligned} U &= \{\text{characters of } \text{Cl}(H_{\mathcal{O}}/K) \text{ which are trivial on } \text{Cl}(H_{\mathcal{O}}/H)\}, \\ V &= \{\text{characters of } \text{Cl}(H_{\mathcal{O}}/H)\}, \\ W &= \{\text{characters of } \text{Cl}(H_{\mathcal{O}}/K)\}, \\ G_k &= \hat{v}_k \circ \iota^{-1}(\pi_{\mathfrak{f}}(\mathbb{Z})^*) \quad (k = 1, \dots, n), \end{aligned}$$

where

$$\hat{v}_k : \prod_{\ell=1}^n \pi_{\mathfrak{p}_{\ell}^{e_{\ell}}}(\mathcal{O}_K)^* \longrightarrow \pi_{\mathfrak{p}_1^{e_1}}(\mathcal{O}_K)^* \times \cdots \times \pi_{\mathfrak{p}_{k-1}^{e_{k-1}}}(\mathcal{O}_K)^* \times \pi_{\mathfrak{p}_{k+1}^{e_{k+1}}}(\mathcal{O}_K)^* \times \cdots \times \pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*$$

is the natural projection which deletes the k -th component. For each character $\psi \in V$, fix a character $\psi' \in W$ which extends ψ (by Lemma 2.4).

(i) *There is a bijective map*

$$\begin{aligned} U \times V &\longrightarrow W \\ (\chi, \psi) &\mapsto \chi \cdot \psi'. \end{aligned}$$

(ii) *We have the inequality*

$$\#\{\xi \in W : \check{\xi}_k = 1\} \leq h_K \frac{\#\pi_{\mathfrak{f}}(\mathcal{O}_K)^*}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \cdot \#G_k} \quad (k = 1, \dots, n).$$

Proof. (i) We see from Lemma 5.1 that both $U \times V$ and W have the same size. Hence it suffices to show that the above map is injective, which is straightforward.

(ii) Without loss of generality it suffices to show that there is an injective map

$$S = \{\xi \in W : \check{\xi}_n = 1\} \longrightarrow U \times \{\text{characters of } \prod_{k=1}^{n-1} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* / G_n\},$$

because $\#U = h_K$ by Lemma 5.1 and $\# \prod_{k=1}^{n-1} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*/G_n = \#\pi_{\mathfrak{f}}(\mathcal{O}_K)^*/(\#\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^* \cdot \#G_n)$.

Let $\xi \in S$. As an element of W , ξ is of the form $\chi \cdot \psi'$ for some $\chi \in U$ and $\psi \in V$ by (i). And, by (5.4) and the fact $\chi \in U$ we get $\check{\chi} = \chi \circ \check{\Psi}_{\mathfrak{f}} = 1$, from which it follows that

$$1 = \check{\xi}_n = (\check{\chi} \cdot \check{\psi}')_n = \check{\psi}'_n. \quad (5.8)$$

We further deduce by (5.4) that

$$\check{\psi}' = \psi'|_{\check{\Psi}_{\mathfrak{f}}(\pi_{\mathfrak{f}}(\mathcal{O}_K)^*)} \circ \check{\Psi}_{\mathfrak{f}} = \psi'|_{\text{Cl}(H_{\mathcal{O}}/H)} \circ \check{\Psi}_{\mathfrak{f}} = \psi \circ \check{\Psi}_{\mathfrak{f}}. \quad (5.9)$$

On the other hand, if β is a character of $\prod_{k=1}^n \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*$ defined by

$$\beta = \psi \circ \check{\Psi}_{\mathfrak{f}} \circ \iota, \quad (5.10)$$

then we derive that

$$\begin{aligned} \beta \circ \iota_n(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*) &= \psi \circ \check{\Psi}_{\mathfrak{f}} \circ \iota \circ \iota_n(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*) \\ &= \check{\psi}' \circ \iota \circ \iota_n(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*) \quad \text{by (5.9)} \\ &= \check{\psi}'_n(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*) = 1 \quad \text{by (5.8),} \end{aligned}$$

which implies

$$\iota_n(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*) \subseteq \text{Ker}(\beta). \quad (5.11)$$

Furthermore, we have $\beta \circ \iota^{-1}(\pi_{\mathfrak{f}}(\mathbb{Z})^*) = \psi \circ \check{\Psi}_{\mathfrak{f}}(\pi_{\mathfrak{f}}(\mathbb{Z})^*) = 1$ by (5.5), which claims

$$\iota^{-1}(\pi_{\mathfrak{f}}(\mathbb{Z})^*) \subseteq \text{Ker}(\beta). \quad (5.12)$$

Hence β can be written as

$$\beta = \gamma \circ \left(\prod_{k=1}^n \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \rightarrow \prod_{k=1}^n \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* / \langle \iota_n(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*), \iota^{-1}(\pi_{\mathfrak{f}}(\mathbb{Z})^*) \rangle \right) \quad (5.13)$$

for a unique character γ of $\prod_{k=1}^n \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* / \langle \iota_n(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*), \iota^{-1}(\pi_{\mathfrak{f}}(\mathbb{Z})^*) \rangle$ by Lemma 5.1, (5.11) and (5.12).

Now, we define a map

$$\begin{aligned} \kappa : S &\longrightarrow U \times \{\text{characters of } \prod_{k=1}^{n-1} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*/G_n\} \\ \xi &\longmapsto (\chi, \gamma \circ \widehat{\iota}_n), \end{aligned}$$

where

$$\widehat{\iota}_n : \prod_{k=1}^{n-1} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*/G_n \longrightarrow \prod_{k=1}^n \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* / \langle \iota_n(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*), \iota^{-1}(\pi_{\mathfrak{f}}(\mathbb{Z})^*) \rangle$$

is definitely a surjection by the definition of G_n . To prove the injectivity of the map κ , assume that $\kappa(\xi_1) = \kappa(\xi_2)$ for some $\xi_1, \xi_2 \in S$. Then, by (i) there are unique $\chi_1, \chi_2 \in U$ and $\psi_1, \psi_2 \in V$ such that $\xi_1 = \chi_1 \cdot \psi'_1$ and $\xi_2 = \chi_2 \cdot \psi'_2$. And, by the definition of κ we get $\chi_1 = \chi_2$. Let ψ_ℓ ($\ell = 1, 2$) induce β_ℓ and γ_ℓ in the above paragraph (which explains β and γ constructed from ψ). Then, since $\widehat{\iota}_n$ is surjective, we obtain $\gamma_1 = \gamma_2$ from the fact $\gamma_1 \circ \widehat{\iota}_n = \gamma_2 \circ \widehat{\iota}_n$, and so we have $\beta_1 = \beta_2$ by (5.13). It then follows from the definition

(5.10), the fact $\psi_1, \psi_2 \in V$ and (5.4) that $\psi_1 = \psi_2$, which concludes the injectivity of κ . This completes the proof. \square

Lemma 5.3. *Let F be a field such that $K \subseteq F \subsetneq H_{\mathcal{O}}$. If*

$$2\#\pi_{\mathfrak{f}}(\mathbb{Z})^* \sum_{k=1}^n \frac{1}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \cdot \#G_k} < 1, \quad (5.14)$$

then there is a character χ of $\text{Cl}(\mathfrak{f})$ such that

$$\chi|_{\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})} = 1, \quad \chi|_{\text{Cl}(K_{\mathfrak{f}}/F)} \neq 1 \quad \text{and} \quad \mathfrak{p}_k | \mathfrak{f}_{\chi} \quad (k = 1, \dots, n). \quad (5.15)$$

Proof. We first derive that

$$\begin{aligned} & \#\{\text{characters } \chi \text{ of } \text{Cl}(\mathfrak{f}) : \chi|_{\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})} = 1, \chi|_{\text{Cl}(K_{\mathfrak{f}}/F)} \neq 1\} \\ &= \#\{\chi \text{ of } \text{Cl}(\mathfrak{f}) : \chi|_{\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})} = 1\} - \#\{\chi \text{ of } \text{Cl}(\mathfrak{f}) : \chi|_{\text{Cl}(K_{\mathfrak{f}}/F)} = 1\} \\ &= \#\text{Cl}(\mathfrak{f})/\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}}) - \#\text{Cl}(\mathfrak{f})/\text{Cl}(K_{\mathfrak{f}}/F) \quad \text{by Lemma 5.1} \\ &= [H_{\mathcal{O}} : K] - [F : K] \\ &= [H_{\mathcal{O}} : K](1 - 1/[H_{\mathcal{O}} : F]) \\ &\geq (1/2)[H_{\mathcal{O}} : K] \quad \text{by the fact } F \subsetneq H_{\mathcal{O}} \\ &= (h_K/2)\#\pi_{\mathfrak{f}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}}(\mathbb{Z})^* \quad \text{from the exact sequence (5.3) and (5.5)} \\ &> h_K\#\pi_{\mathfrak{f}}(\mathcal{O}_K)^* \sum_{k=1}^n \frac{1}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \cdot \#G_k} \quad \text{by the assumption (5.14).} \end{aligned}$$

On the other hand, we find that

$$\begin{aligned} & \#\{\chi \text{ of } \text{Cl}(\mathfrak{f}) : \chi|_{\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})} = 1, \mathfrak{p}_k \nmid \mathfrak{f}_{\chi} \text{ for some } k\} \\ &\leq \#\{\chi \text{ of } \text{Cl}(\mathfrak{f}) : \chi|_{\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})} = 1, \tilde{\chi}_k = 1 \text{ for some } k\} \quad \text{by Lemma 2.1} \\ &= \#\{\xi \text{ of } \text{Cl}(H_{\mathcal{O}}/K) : \tilde{\xi}_k = 1 \text{ for some } k\} \quad \text{by the argument followed by Lemma 5.1} \\ &\leq h_K\#\pi_{\mathfrak{f}}(\mathcal{O}_K)^* \sum_{k=1}^n \frac{1}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \cdot \#G_k} \quad \text{by Lemma 5.2(ii).} \end{aligned}$$

Therefore, there exists a character χ of $\text{Cl}(\mathfrak{f})$ which satisfies the condition (5.15). \square

Theorem 5.4. *If $\mathfrak{f} = N\mathcal{O}_K$ satisfies the assumption (5.14) in Lemma 5.3, then the singular value in (4.1) generates $H_{\mathcal{O}}$ over K as a real algebraic integer.*

Proof. Let $\varepsilon = \mathbf{N}_{K_{\mathfrak{f}}/H_{\mathcal{O}}}(g_{\mathfrak{f}}(C_0))$ and $F = K(\varepsilon)$ as a subfield of $H_{\mathcal{O}}$. Suppose that F is properly contained in $H_{\mathcal{O}}$, then there is a character χ of $\text{Cl}(\mathfrak{f})$ satisfying the condition (5.15) in Lemma 5.3. Since $\mathfrak{p}_k | \mathfrak{f}_k$ for all $k = 1, \dots, n$, the Euler factor of χ in Proposition 2.2 is 1, and hence the value $S_{\mathfrak{f}}(\overline{\chi}, g_{\mathfrak{f}})$ does not vanish by Remark 2.3(ii). On the other hand, we can derive $S_{\mathfrak{f}}(\overline{\chi}, g_{\mathfrak{f}}) = 0$ by using the condition (5.15) of χ in exactly the same way as the proof of Theorem 2.7, which gives rise to a contradiction. Therefore $H_{\mathcal{O}} = K(\varepsilon)$, and hence we can apply the argument of Theorem 4.2 to complete the proof. \square

Remark 5.5. Let $N (\geq 2)$ be an integer with prime factorization

$$N = \prod_{a=1}^A s_a^{u_a} \prod_{b=1}^B q_b^{v_b} \prod_{c=1}^C r_c^{w_c},$$

where each s_a (respectively, q_b and r_c) splits (respectively, is inert and ramified) in K/\mathbb{Q} . Then we have the prime ideal factorization

$$\mathfrak{f} = N\mathcal{O}_K = \prod_{a=1}^A (\mathfrak{s}_a \bar{\mathfrak{s}}_a)^{u_a} \prod_{b=1}^B \mathfrak{q}_b^{v_b} \prod_{c=1}^C \mathfrak{r}_c^{2w_c}$$

with

$$\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{s}_a) = \mathbf{N}_{K/\mathbb{Q}}(\bar{\mathfrak{s}}_a) = s_a, \quad \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{q}_b) = q_b^2, \quad \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{r}_c) = r_c.$$

Now, for the sake of convenience, we let

$$\mathfrak{f} = \prod_{k=1}^{2A+B+C} \mathfrak{p}_k^{e_k}$$

with

$$(\mathfrak{p}_k, e_k) = \begin{cases} (\mathfrak{s}_k, u_k) & \text{for } k = 1, \dots, A \\ (\bar{\mathfrak{s}}_{k-A}, u_{k-A}) & \text{for } k = A+1, \dots, 2A \\ (\mathfrak{q}_{k-2A}, v_{k-2A}) & \text{for } k = 2A+1, \dots, 2A+B \\ (\mathfrak{r}_{k-2A-B}, 2w_{k-2A-B}) & \text{for } k = 2A+B+1, \dots, 2A+B+C, \end{cases} \quad (5.16)$$

and consider the surjection

$$\mu_k = \widehat{v}_k \circ \iota^{-1} : \pi_{\mathfrak{f}}(\mathbb{Z})^* \longrightarrow G_k (\subseteq \pi_{\mathfrak{p}_1^{e_1}}(\mathcal{O}_K)^* \times \dots \times \pi_{\mathfrak{p}_{k-1}^{e_{k-1}}}(\mathcal{O}_K)^* \times \pi_{\mathfrak{p}_{k+1}^{e_{k+1}}}(\mathcal{O}_K)^* \times \dots \times \pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*).$$

If $m \pmod{\mathfrak{f}} \in \pi_{\mathfrak{f}}(\mathbb{Z})^*$ belongs to $\text{Ker}(\mu_k)$, then

$$\begin{aligned} \underbrace{(1, \dots, 1)}_{n-1} &= \mu_k(m \pmod{\mathfrak{f}}) = \widehat{v}_k \circ \iota^{-1}(m \pmod{\mathfrak{f}}) \\ &= (m \pmod{\mathfrak{p}_1^{e_1}}, \dots, m \pmod{\mathfrak{p}_{k-1}^{e_{k-1}}}, m \pmod{\mathfrak{p}_{k+1}^{e_{k+1}}}, \dots, m \pmod{\mathfrak{p}_n^{e_n}}), \end{aligned} \quad (5.17)$$

which shows

$$\iota^{-1}(\text{Ker}(\mu_k)) \subseteq \iota_k(\pi_{\mathfrak{p}_k^{e_k}}(\mathbb{Z})^*) = \{(1, \dots, 1, t \pmod{\mathfrak{p}_k^{e_k}}, 1, \dots, 1) : t \in \mathbb{Z} \text{ which is prime to } \mathfrak{p}_k\}.$$

Hence, this gives the inequality

$$\#G_k = \frac{\#\pi_{\mathfrak{f}}(\mathbb{Z})^*}{\#\text{Ker}(\mu_k)} \geq \frac{\#\pi_{\mathfrak{f}}(\mathbb{Z})^*}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathbb{Z})^*}. \quad (5.18)$$

In particular, if $k = 1, \dots, 2A$, then μ_k becomes injective (and so, bijective). Indeed, if $m \pmod{\mathfrak{f}} \in \pi_{\mathfrak{f}}(\mathbb{Z})^*$ belongs to $\text{Ker}(\mu_k)$, then

$$m \equiv 1 \pmod{\mathfrak{p}_\ell^{e_\ell}} \quad \text{for } \ell \neq k \quad (5.19)$$

by (5.17). But, since m is an integer, (5.19) implies

$$m \equiv 1 \pmod{\bar{\mathfrak{p}}_\ell^{e_\ell}} \quad \text{for } \ell \neq k. \quad (5.20)$$

On the other hand, since $\mathfrak{p}_k = \bar{\mathfrak{p}}_{k+A}$ or $\bar{\mathfrak{p}}_{k-A}$ by the definition (5.16), we deduce by (5.19) and (5.20) that

$$m \equiv 1 \pmod{\mathfrak{p}_\ell^{e_\ell}} \quad \text{for all } \ell = 1, \dots, n,$$

from which we get $m \equiv 1 \pmod{\mathfrak{f}}$. This concludes that μ_k is injective; hence

$$\#G_k = \#\pi_{\mathfrak{f}}(\mathbb{Z})^* \quad \text{for } k = 1, \dots, 2A. \quad (5.21)$$

Thus we achieve by (5.18), (5.21) and the Euler functions for integers and ideals that

$$(\text{LHS}) \text{ of (5.14)} \leq 4 \sum_{a=1}^A \frac{1}{(s_a - 1)s_a^{u_a-1}} + 2 \sum_{b=1}^B \frac{1}{(q_b + 1)q_b^{v_b-1}} + 2 \sum_{c=1}^C \frac{1}{r_c^{w_c}}.$$

Therefore, one can also apply Theorem 5.4 under the assumption

$$4 \sum_{a=1}^A \frac{1}{(s_a - 1)s_a^{u_a-1}} + 2 \sum_{b=1}^B \frac{1}{(q_b + 1)q_b^{v_b-1}} + 2 \sum_{c=1}^C \frac{1}{r_c^{w_c}} < 1. \quad (5.22)$$

Example 5.6. Let $K = \mathbb{Q}(\sqrt{-2})$ and \mathcal{O} be the order of conductor $N = 9 (= 3^2)$ in K . Then, $N\mathcal{O}_K$ satisfies the assumption (5.22) in Remark 5.5 (but, not the assumption (2.3) in Lemma 2.5), and hence the singular value $3^{12}\Delta(9\theta)/\Delta(3\theta)$ with $\theta = \sqrt{-2}$ generates $H_{\mathcal{O}}$ over K by Theorem 5.4. Since $h_K = 1$ ([4, p.29]), one can estimate its minimal polynomial in exactly the same way as Example 4.4:

$$\begin{aligned} & \min(3^{12}\Delta(9\theta)/\Delta(3\theta), K) \\ &= X^6 + 52079706X^5 + 2739284675932815X^4 + 12787916715651570220X^3 \\ & \quad + 190732505724302106460815X^2 - 268398119546256294X + 1. \end{aligned}$$

REFERENCES

1. I. Chen and N. Yui, *Singular values of Thompson series*, Groups, difference sets, and the Monster (Columbus, OH, 1993), 255–326, Ohio State Univ. Math. Res. Inst. Publ. 4, Walter de Gruyter, Berlin, 1996.
2. B. Cho and J. K. Koo, *Construction of class fields over imaginary quadratic fields and applications*, Quart. J. Math. (2010) 61 (2), 199–216.
3. H. Cohen, *Advanced Topics in Computational Number Theory*, Grad. Texts in Math. 193, Springer-Verlag, New York, 2000.
4. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., New York, 1989.
5. D. A. Cox, J. McKay and P. Stevenhagen, *Principal moduli and class fields*, Bull. London Math. Soc. 36 (2004), no. 1, 3–12.
6. G. J. Janusz, *Algebraic Number Fields*, 2nd edition, Grad. Studies in Math. 7, Amer. Math. Soc., Providence, R. I., 1996.
7. H. Y. Jung, J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions (II)*, <http://arxiv.org/abs/1007.2318>, submitted.
8. J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit. 264 (2010) 137–177.
9. J. K. Koo and D. H. Shin, *Function fields of certain arithmetic curves and application*, Acta Arith. 141 (2010), no. 4, 321–334.
10. D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Springer-Verlag, 1981.

11. S. Lang, *Algebraic Number Theory*, 2nd edition, Grad. Texts in Math. 110, Springer-Verlag, New York, 1994.
12. S. Lang, *Elliptic Functions*, With an appendix by J. Tate, 2nd edition, Grad. Texts in Math. 112, Springer-Verlag, New York, 1987.
13. K. Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math. (2) 80(1964), 104–148.
14. R. Schertz, *Construction of ray class fields by elliptic units*, J. Théor. Nombres Bordeaux 9 (1997), no. 2, 383–394.
15. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, Princeton, N. J., 1971.
16. P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class Field Theory-Its Centenary and Prospect (Tokyo, 1998), 161–176, Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001.

DEPARTMENT OF MATHEMATICAL SCIENCES, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: zandc@kaist.ac.kr

DEPARTMENT OF MATHEMATICAL SCIENCES, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: jkkoo@math.kaist.ac.kr

DEPARTMENT OF MATHEMATICAL SCIENCES, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: shakur01@kaist.ac.kr